No. 23-7597-cv

United States Court of Appeals for the Second Circuit

DETRINA SOLOMON, on behalf of herself and all others similarly situated, *Plaintiff-Appellant*,

v.

FLIPPS MEDIA, INC., DBA FITE, DBA FITE TV, Defendant-Appellee.

On Appeal From the United States District Court for the Eastern District of New York

PETITION FOR REHEARING EN BANC

NICOMEDES S. HERRERA BRET D. HEMBD HERRERA KENNEDY LLP 1300 Clay Street, Suite 600 Oakland, California 94612 (510) 422-4700

CHRISTOPHER J. CORMIER BURNS CHAREST LLP 4725 Wisconsin Ave. NW, Suite 200 Washington, DC 20016 (202) 577-3977

Dated: June 11, 2025

CHARLES GERSTEIN
(counsel of record)
JASON HARROW
JEREMY SHUR
GERSTEIN HARROW LLP
400 7th Street NW, Suite 304
Washington, DC 20025
(202) 670-4809
charlie@gerstein-harrow.com

Attorneys for Plaintiff-Appellant Detrina Solomon

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017) 7, 8, 15, 17 In re Nickelodeon Consumer Priv. Litig., 827 F.3d 262 (3d Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC, Manza v. Pesi, Inc., No. 24-CV-690-JDP, 2025 WL 1445762 Salazar v. Nat'l Basketball Ass'n, 118 F.4th 533 (2d Cir. Solomon v. Flipps Media, Inc., 136 F.4th 41 (2nd Cir. 2025) passim Yershov v. Gannett Satellite Information Network, Incorporated, 820 F.3d 482 (1st Cir. 2016)......passim Statutes Other Authorities C. Suetonius Tranquillus, Life of Julius Caesar, in THE LIVES OF THE TWELVE CAESARS (Alexander Thomson CENTRAL TIBETAN ADMINISTRATION, BASELINE STUDY OF THE TIBETAN DIASPORA COMMUNITY OUTSIDE SOUTH

LOKKER, Online Data Privacy Report: March 2024 at 3 (March 2024), https://lokker.com/online-data-privacy-report-march-2024/.	5
Michael Dolan, <i>The Bork Tapes</i> , WASH. CITY PAPER (Sept. 25–Oct. 1, 1987), <i>available at</i> https://perma.cc/37V2-T2ZD	16
S. P.N.1107, 116th Congress (Nov. 7, 2019)	14
S. REP. 599, 2, 1988 U.S.C.C.A.N. 4342-1	3, 18

PRELIMINARY STATEMENT

The Video Privacy Protection Act (VPPA) forbids a "video tape service provider" to disclose "personally identifiable information," defined to "include[] information which identifies a person as having requested or obtained specific video materials or services . . . ," to any other person without the requester's consent. 18 U.S.C. § 2710(a)(3), (b)(2).

The Panel in this case held that a video tape service provider may disclose a specific requester's video-viewing history in complete detail to a third party so long as the service provider sends it in a form that would not be readable to an "ordinary person," even if the service provider knows that the recipient can and will understand that information and use it to identify the requester. Solomon v. Flipps Media, Inc., 136 F.4th 41, 52 (2nd Cir. 2025). This holding is in direct and acknowledged conflict with Yershov v. Gannett Satellite Information Network, Incorporated, 820 F.3d 482, 486 (1st Cir. 2016), and it is wrong as a matter of the plain meaning and clear purpose of the Act. If the Panel's rule prevails, the video clerk who inspired the Act's passage by disclosing Judge Robert Bork's video-rental history to the Washington City Paper need only have used a simple code, or a foreign language: Because an "ordinary person"

would not know the code or speak the language, but the *City Paper* reporter would, the clerk could subvert the entire function of the law with trivial ease. That cannot be right.

The "ordinary person" standard creates a loophole that is unsupported by the statutory text and contrary to the purpose of the statute—a loophole that companies are exploiting to provide granular information about their users' video watching to Facebook without those users' consent. To correct this error, this Court should grant rehearing en banc because the Panel decision conflicts with an authoritative decision of another circuit.

BACKGROUND

The VPPA was enacted in 1987 in response to a video-store clerk telling the Washington *City Paper* which videos then—Supreme Court nominee Judge Robert Bork's family had rented. *Solomon*, 136 F.4th at 43. Under the VPPA, a "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person" 18 U.S.C. § 2710(b)(1). "The term 'personally identifiable information' includes information which identifies a person as having requested or

obtained specific video materials from a video tape service provider." *Id.* (a)(3). Although "[t]he classic example [of a VPPA violation] will always be a video clerk leaking an individual customer's video rental history," *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 290 (3d Cir. 2016), there is no question that Congress specifically understood the Act to apply to disclosures of online viewing information: Congress amended the Act in 2013 to allow consent to be given online, keeping in place the rest of the statute. *Id.* at 277.

Indeed the VPPA was drafted in the first instance with the expansion of technological tracking of consumers in mind. Congress was concerned that in a technological era in which consumer activities are "all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what . . . sort of television programs they watch," which members likened to "Big Brother." S. REP. 599, 2, 1988 U.S.C.C.A.N. 4342-1, 4342-1 at 5–6. The Senate also cited Supreme Court opinions in which the Court "warned of the danger that new technologies would chip away at traditional privacy safeguards" and of "the threat to privacy implicit in the accumulation of vast amounts of

personal information in computerized data banks." *Id.* at 4–5 (citations omitted).

This case is one of several alleging that online video providers use a piece of computer code called the "Meta Pixel" to send their customers' video-viewing history to Meta Platforms, Inc., formerly known (and referred to here) as Facebook, to do what the Senate feared. *E.g.*, *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 538 (2d Cir. 2024). The Meta Pixel is a piece of software code that Facebook offers to websites. JA16 ¶ 43. When a user accesses a website with a Pixel installed, the Pixel, operating in the background, sends a message to Facebook about the user's interaction with the website. *Id.*

Facebook's business model requires that it be able to track users' activity and link it to known facts about those users. To do this, Facebook uses common pieces of software called "cookies." A cookie is a small block of data placed on the user's computer or web browser while the user browses a website. E.g., JA18 ¶ 50. Any time uses visit Facebook or any associated site, cookies are sent to the users' browsers by which Facebook can subsequently identify them if they return to any Facebook website.

JA23 ¶ 65. People who use Facebook or Instagram are sent a cookie that will immediately link them to the their personal accounts. Id.

Facebook uses these cookies to link the information it gathers from the Pixel with Facebook and Instagram accounts. Users with Facebook accounts are assigned a "c_user" cookie, which corresponds to their Facebook ID, a unique number identifying their Facebook profile. JA19 \P 55. Although the transmission itself is written in computer code, JA 22¶ 64 (example code), any person armed with a user's c_user cookie can identify that user's Facebook page by typing "www.facebook.com/[c-user cookie]" with that user's c_user cookie number, JA21 ¶ 62. The upshot of this is that nearly half of retail websites send to Facebook information that Facebook can use to identify the person who has interacted with the website. E.g., Lokker, Online Data Privacy Report: March 2024 at 3 https://lokker.com/online-data-privacy-report-march-(March 2024), 2024/.

Defendant Flipps Media, Inc., doing business as "FITE," operates a website on which subscribers can view pre-recorded videos. JA8 ¶ 2. Plaintiff-Appellant Detrina Solomon alleged that she watched videos on the FITE website, JA32 ¶¶ 105–07, and that whenever she watched a

video, FITE used a c_user cookie on her browser to send the video's title to Facebook alongside her Facebook ID. JA32 ¶ 107.

There is no question that Facebook could use this information to identify Solomon as having watched specific videos on FITE nor that FITE sent this information to Facebook for that purpose, and there is also no question that an ordinary person reading the computer code that FITE sent to Facebook would find that text incomprehensible. *E.g.* JA 22 ¶ 64.

Solomon sued FITE alleging violations of the VPPA. JA8–35 (complaint). The district court (Azrack, J.) dismissed Solomon's complaint, holding that (a) the messages FITE sent to Facebook were not "personally identifiable information" because an "ordinary person" could not use them to identify Solomon as having watched videos, JA4–5, and (b) Solomon had not plausibly alleged that she had watched "prerecorded" videos because, although she alleged that FITE offered both pre-recorded and live videos, and although she had alleged that she watched videos on FITE, it was *implausible* to infer that Solomon had watched pre-recorded videos "given the preference of many viewers to watch sporting events 'live." JA124. The district court then denied

Solomon leave to amend, reasoning that Solomon had sufficient opportunity to amend because FITE had filed a pre-motion letter, JA124.

Solomon timely appealed, JA128, and the Panel (Raggi, Chin, and Nardini, JJ.) affirmed. The Panel adopted the "ordinary person" standard for personally identifiable information, see Eichenberger v. ESPN, Inc., 876 F.3d 979, 984 (9th Cir. 2017), and rejected the "reasonable foreseeability" standard, see Yershov, 820 F.3d at 486. It then held that Solomon had not alleged that FITE had transmitted to Facebook information with which an ordinary person could identify her because the transmission was in code. Solomon, 136 F.4th at 48–50, 51. The Panel thus did not address whether Solomon had plausibly alleged that she had watched pre-recorded videos, and affirmed the dismissal with prejudice. Since the decision, the Panel's reasoning has been rejected by a district court, which concluded that the Panel did not "rely on the text" of the VPPA. Manza v. Pesi, Inc., No. 24-CV-690-JDP, 2025 WL 1445762, at *6 (W.D. Wis. May 20, 2025).

ARGUMENT

The Panel decision conflicts with the First Circuit's decision in Yershov, 820 F.3d 482. This Court should grant rehearing en banc, vacate

the Panel's decision, adopt the First Circuit's better-reasoned decision, and remand to the district court for further proceedings. *See* FRAP 40(b)(2)(C) (providing for rehearing en banc when "the panel decision conflicts with an authoritative decision of another United States court of appeals").

I. The Panel Decision Puts This Circuit in Direct and Acknowledged Conflict With the First Circuit

The courts of appeals have read the VPPA's definition of "personally identifiable information" in two ways: the "reasonable foreseeability standard," under which information qualifies as "personally identifiable" if it is "reasonably and foreseeably likely to reveal which . . . videos [someone] has obtained," Yershov, 820 F.3d at 486; and the "ordinary person" standard, under which information qualifies as "personally identifiable" if it "readily permit[s] an ordinary person to identify a specific individual's video-watching behavior," Eichenberger, 876 F.3d at 985 (quoting Nickelodeon, 827 F.3d at 267). Here, the Panel agreed with Eichenberger and Nickelodeon and rejected Yershov, and under the rule in Yershov the Panel would have ruled for Solomon.

In *Nickelodeon*, the Third Circuit considered whether the owner of a website offering children's videos violated the VPPA by disclosing to

Google information linking video titles to (a) "a user's IP address," which is "a number assigned to each device that is connected to the Internet that permits computer-specific online tracking," 827 F.3d at 281 (quotation omitted); (b) "a user's browser and operating system settings, which comprise a so-called 'browser fingerprint," id. at 281–82; and (c) a computing device's "unique device identifier," id. at 281. The Third Circuit held that even though Google could use that information to "track the same computer across time," that information was not "personally identifiable" because "[t]o an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person." Id. at 283.

The First Circuit read the statute differently. In Yershov, it considered whether a website operator violated the VPPA by disclosing to Adobe, an internet-services company, "(1) the title of the video viewed, (2) the GPS coordinates of the device at the time the video was viewed, and (3) certain identifiers associated with the user's device." 820 F.3d at 484. The First Circuit ruled for the plaintiffs. It used the metaphor of "a football referee announc[ing] a violation by 'No. 12 on the offense," which is incomprehensible to the ordinary listener but "everyone with a game

program knows the name of the player who was flagged." *Id.* at 486. So too was the information sent to Adobe "personally identifiable" because when the website "makes such a disclosure to Adobe, it knows that Adobe has the 'game program,' so to speak." *Id.* at 486.

Finally, in *Eichenberger*, the Ninth Circuit considered whether ESPN violated the VPPA when it "knowingly disclosed to . . . Adobe Analytics: (1) Plaintiff's . . . device serial number and (2) the identity of the video that he watched." 876 F.3d at 981. The Ninth Circuit explained that "[t]wo circuits have considered that question in similar cases," *id*. (citing *Nickelodeon*, 827 F.3d at 281, and *Yershov*, 820 F.3d at 484), "and each has articulated a different standard," *id*. The court then "adopt[ed] the Third Circuit's 'ordinary person' standard" and held that the information ESPN disclosed to Adobe was not "personally identifiable" because an ordinary person would not be able to use it to identify the viewer. *Id*. at 985.

The Panel in this case rejected the First Circuit's holding. *Solomon*, 136 F.4th at 48–50. The complaint in this case alleges facts giving rise to a plausible inference that FITE sent information to Facebook that FITE *intended* Facebook to use to identify Solomon for targeted advertising, JA

32 ¶ 107, and that Facebook so used it, thus satisfying the standard in Yershov. But the complaint also makes clear that (a) an ordinary person receiving that message would see only incomprehensible computer code, JA 22 ¶ 64, and (b) even an ordinary person who could understand computer code would not necessarily know the name of the person watching videos, thus failing the "ordinary person" standard. Solomon, 136 F.4th at 54 ("It is implausible that an ordinary person would look at the phrase 'title% 22% 3A% 22-% E2% 96% B7% 20The% 20Roast% 20of% - 20Ric% 20Flair' . . . and understand it to be a video title."); id. "Nor does the Complaint plausibly allege that an ordinary person could identify Solomon through her FID [Facebook ID]."). The Panel decision thus squarely conflicts with an authoritative decision of the First Circuit, and this Court should grant rehearing en banc.

II. The Panel's Decision is Wrong

The Panel's decision and the cases on which it relies depart from the plain meaning of the VPPA. See Manza v. Pesi, Inc., No. 24-CV-690-JDP, 2025 WL 1445762, at *6 (W.D. Wis. May 20, 2025) (noting that Solomon does not "rely on the text" of the VPPA and calling its reasons for the departure "not persuasive"). The Panel reasoned that information

must be "personally identifiable" or not no matter the recipient, even though the statute focuses on "knowing disclos[ure]," which necessarily depends on there being a recipient who can understand the disclosure.

The VPPA reads, in relevant part:

A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person.

* * *

[T]he term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

18 U.S.C. § 2710(b)(1), (a)(3). The plain text thus requires that there be at least two people in any "disclosure": (1) the sender, a "video tape service provider" who "knowingly discloses" information, and (2) "any person," "to" whom the information is sent. *Id.* (b)(1). The word "disclose" necessarily requires a recipient who can understand a piece of information. *See*, *e.g.*, BLACK'S LAW DICTIONARY, *Disclose* ("To make (something) *known* . . . "). The "disclos[ure]" of "personally identifiable information" "to any person" thus necessarily depends on there being a

person who understands that information; one cannot "disclose" information to a potato.

The first mistake in adopting the "ordinary person" standard is thus the conclusion, without meaningful support, that "18 U.S.C. § 2710(b) . . . views disclosure from the perspective of the disclosing party. . . . As a result, 'personally identifiable information' must have the same meaning without regard to its recipient's capabilities." *Eichenberger*, 876 F.3d at 985; *see also Solomon*, 136 F.4th at 52 ("It does not make sense that a video tape service provider's liability would turn on circumstances outside of its control and the level of sophistication of the third party."). This reading makes a hash out of the word "disclose." "Disclosure," as explained above, happens only if someone receives a piece of information, an inquiry that necessarily depends on "the level of sophistication" of the recipient. *Id*.

And anyway there is no reason to believe that the third party's "level of sophistication" is "outside of [the service provider's] control." *Id.*A video tape service provider who sends encrypted information to someone the provider incorrectly believes to be incapable of reading it has not *knowingly* disclosed information; but a provider who sends

encrypted information that an ordinary person could not read to someone the provider knows *can* read it *has* knowingly disclosed information. The person to whom someone knowingly sends a message is very much within the sender's "control," and so it makes sense that whether information is "personally identifiable" depends, in part, on who receives it.

The Panel also erred by conflating at least two senses in which a piece of information can be more or less "identifiable" of a specific person's relationship to a specific video. First, information can identify a person in a way that is more or less specific to that person. One could say, in ascending order of specificity, (a) an active-duty judge of the United States Court of Appeals for the Second Circuit (13 possibilities), (b) an active-duty judge of the Second Circuit whose surname begins with "N" (two possibilities) or (c) an active-duty judge of the Second Circuit who was confirmed by the Senate on November 7, 2019 (one possibility). Second, information can be more or less comprehensible as information. To readers of this brief, the person in (c) above is easily identifiable as The Honorable William Joseph Nardini, of Connecticut, see S. P.N.1107, 116th Congress (Nov. 7, 2019), but few "ordinary" people would be able to use the information to identify Judge Nardini.

Similarly, "Xli Lsrsvefpi Amppmeq Nswitl Revhmrm, sj Gsrrigxmgyx" is almost certainly incomprehensible to most readers of this brief, but to readers of this brief who know that it is encoded with Ceaser's cipher, it immediately identifies Judge Nardini. See C. Suetonius Tranquillus, Life of Julius Caesar, in The Lives of the Twelve Caesars § 56 (Alexander Thomson ed. 1883) ("If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet.").

The Ninth Circuit's standard in *Eichenberger*, for example, uses "identifiable" in the first sense:

The manager of a video rental store in Los Angeles understood that if he or she disclosed the name and address of a customer . . . the recipient of that information could identify the customer. By contrast, it was clear that, if the disclosure were that 'a local high school teacher' had rented a particular movie, the manager would not have violated the statute.

Eichenberger, 876 F.3d at 985. But the Panel appears to use "identifiable" in the second sense—comprehensibility. The Panel reasoned that FITE's disclosure to Facebook was not "personally identifiable" because "[i]t is

implausible that an ordinary person would look at the phrase 'title% 22% 3A% 22-% E2% 96% B7% 20The% 20Roast% 20of% 20Ric% 20Flair'... and understand it to be a video title" and because "[t]he Complaint is devoid of any details about how an ordinary person would use an FID to identify Solomon." *Solomon*, 136 F.4th at 54.

The Panel's decision thus leads to the remarkable conclusion that the VPPA would not be violated if a video store clerk sent "Vsfivx Fsvo, Xli Qer Als Oria Xss Qygl" to a reporter after telling the reporter "I used Caeser's cipher," even though the reporter would then immediately know that Robert Bork rented The Man Who Knew Too Much. See Michael Dolan, The Bork Tapes, WASH. CITY PAPER (Sept. 25-Oct. 1, 1987), available at https://perma.cc/37V2-T2ZD. Under the Panel's reasoning, only information that is comprehensible to an "ordinary person" counts, and the cipher text above is not comprehensible to an ordinary person. But in any plain-meaning sense of the words "disclose" and "information which identifies a person as having requested or obtained specific video materials" the video-store clerk using a cipher "disclosed" that Judge Bork rented The Man Who Knew Too Much. The Panel's decision thus

cannot be right—it causes the plain text of the law to reach the opposite of what it surely meant when it was drafted.

What's more, it is unclear what an "ordinary person" knows. Does an "ordinary person" know, for example, who the circuit justice of the Second Circuit is? Would a message in Tibetan be comprehensible to an "ordinary person" in the United States? What about to someone in Jackson Heights, Queens, home to the largest Tibetan-speaking population in the United States? See, e.g., Central Tibetan Administration, Baseline Study of the Tibetan Diaspora Community Outside South Asia 45 (2020). On the Panel's logic, a video tape service provider's liability may depend on how common or uncommon certain knowledge is, which may be beyond the service provider's ability to predict. Contra Solomon, 136 F.4th at 52.

The reasonable-foreseeability test better comports with the statute's text and avoids these problems. After all, the statute requires that one "knowingly disclose[]" information, which necessarily denotes the intent to communicate to a recipient. And there is no reason to believe that the reasonable-foreseeability test takes the law any farther from the "circumstances . . . that motivated its passage," *Eichenberger*, 876 F.3d

at 985, which would in any event yield to the plain text, e.g., Bostock v. Clayton County, 590 U.S. 644, 653 (2020). When Congress passed the VPPA, it was concerned with exactly what happened here: "new technologies" "chip[ping] away at traditional privacy safeguards" by the "accumulation of vast amounts of personal information in computerized data banks." S. REP. 599, 2, 1988 U.S.C.C.A.N. 4342-1, 4342-1 at 4–5 (citations omitted). The data in those computer banks was as incomprehensible to the ordinary person in 1988 as it is today, and it was as personally identifying too.

CONCLUSION

For the foregoing reasons, this Court should grant rehearing en banc, adopt the better-reasoned reasonable-foreseeability test, and remand this case for further proceedings in the district court.

¹ In particular, the court should also remand with instructions that Plaintiff be permitted to amend the Complaint. It was an additional error for the Panel to affirm the dismissal of the complaint with prejudice when amendment could have corrected the other error identified by the district court, and the Plaintiff did not have the benefit of any court decision before the case was dismissed with prejudice. See Loreley Fin. (Jersey) No. 3 Ltd. v. Wells Fargo Sec., LLC, 797 F.3d 160, 190 (2d Cir. 2015) (merely seeing argument in a defendant's pre-motion letter was not sufficient notice to permit a district court to dismiss with prejudice, because "[w]ithout the benefit of a [court] ruling, many a plaintiff will not

Dated: June 11, 2025

Respectfully submitted,

/s/ Charles Gerstein
CHARLES GERSTEIN
JASON HARROW
JEREMY SHUR
GERSTEIN HARROW LLP
400 7th Street NW, Suite 304
Washington, DC 20025
(202) 670-4809
charlie@gerstein-harrow.com

NICOMEDES S. HERRERA BRET D. HEMBD HERRERA KENNEDY LLP 1300 Clay Street, Suite 600 Oakland, California 94612 (510) 422-4700

CHRISTOPHER J. CORMIER BURNS CHAREST LLP 4725 Wisconsin Ave. NW, Suite 200 Washington, DC 20016 (202) 577-3977

Attorneys for Plaintiff-Appellant Detrina Solomon

see the necessity of amendment or be in a position to weigh the practicality and possible means of curing specific deficiencies").

CERTIFICATE OF COMPLIANCE

This motion complies with the type-volume limitation of Federal

Rule of Appellate Procedure 40(d)(3) because this brief contains 3,720

words, excluding the parts of the brief exempted by Federal Rule of

Appellate Procedure 32(f). This brief complies with the typeface

requirements of Rule 32(a)(5) and the type-style requirements of Rule

32(a)(6) because it has been prepared in proportionally spaced typeface

20

using Microsoft Word 365 in 14-point Century Schoolbook font.

/s/ Charles Gerstein

Counsel for appellant

June 11, 2025